ASA 8.3 以降：DMZ でのメール（SMTP）サーバ アクセスの設定例

内容

概要

この設定例は、Demilitarized Zone（DMZ; 緩衝地帯）ネットワークに配置された Simple Mail Transfer Protocol（SMTP）サーバにアクセスするために ASA セキュリティ アプライアンスを設定する方法を示します。

バージョン 8.3 以降の Cisco Adaptive Security Appliance（ASA）での ASDM を使用した同等な設定の詳細について『ASA 8.3.x 以降：内部ネットワーク上のメール（SMTP）サーバ アクセスの設定例」を参照してください。

バージョン 8.3 以降の Cisco Adaptive Security Appliance（ASA）での ASDM を使用した同等な設定の詳細について『ASA 8.3.x 以降：外部ネットワーク上のメール（SMTP）サーバ アクセスの設定例」を参照してください。

Cisco 適応型セキュリティ アプライアンス（ASA）バージョン 8.2 以降の同等設定については、「PIX/ASA 7.x 以降：DMZ でのメール（SMTP）サーバ アクセスの設定例」を参照してください。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- バージョン 8.3 以降が稼働する Cisco 適応型セキュリティ アプライアンス（ASA）
- Cisco 1841 ルータ（Cisco IOS® Software Release 12.4(20)T 搭載）

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『シスコ テクニカル ティップスの表記法』を参照してください。

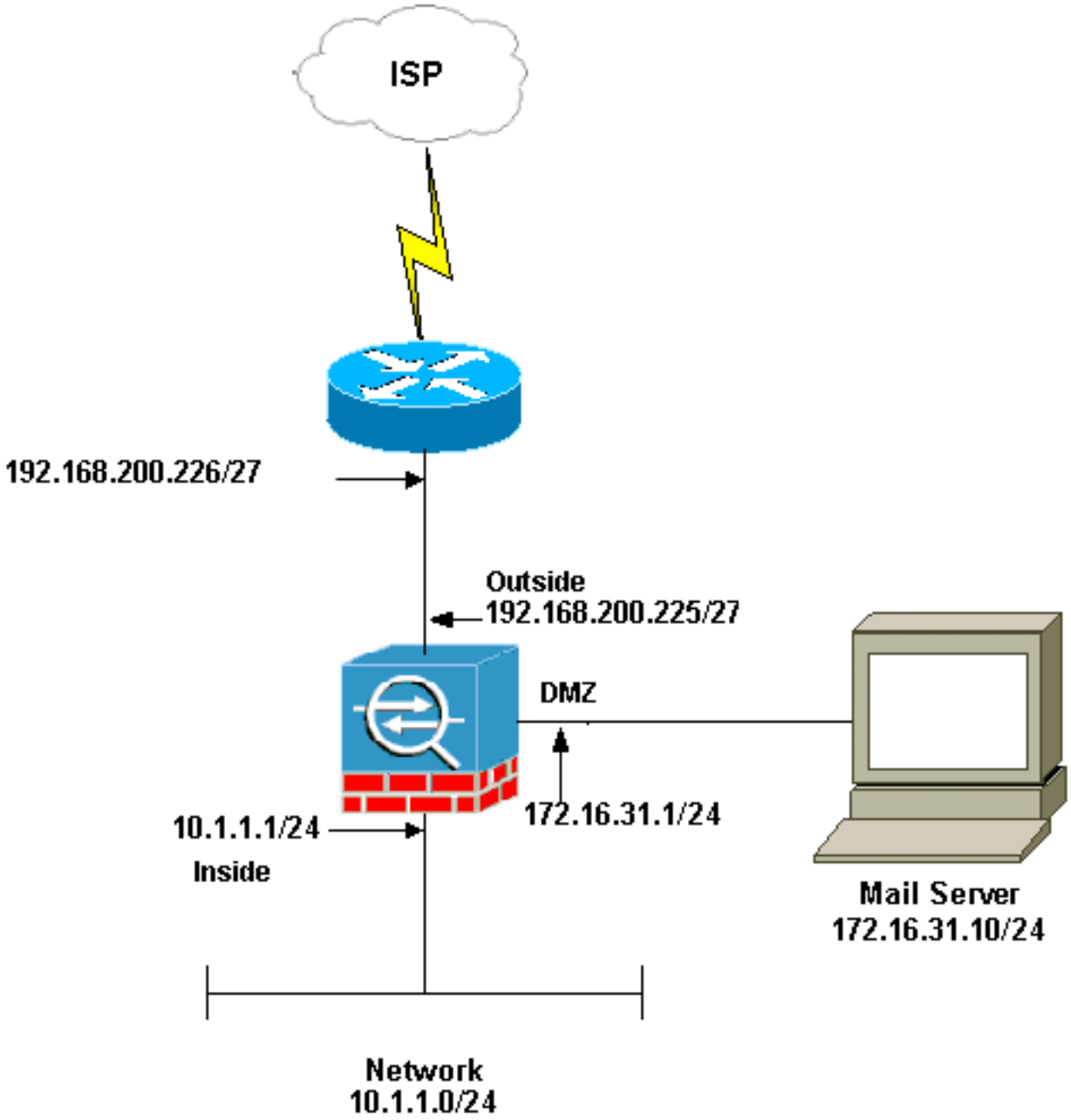
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を参照してください。一部ツールについては、ゲスト登録のお客様にはアクセスできない場合がありますことをご了承ください。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



注：この設定で使用されるIPアドレッシング方式は、インターネット上で正式にルーティング可能なものではありません。これらは RFC 1918 で使用されているアドレスであり、ラボ環境で使用されたものです。

この例で使用しているネットワーク構成の ASA には、内部ネットワーク（10.1.1.0/24）と外部ネットワーク（192.168.200.0/27）があります。 IP アドレス 172.16.31.10 のメール サーバは Demilitarized Zone（DMZ; 緩衝地帯）ネットワークに配置されています。内部からアクセスされるメール サーバについては、ユーザがアイデンティティ NAT を設定します。メール サーバから内部ネットワーク内のホストへの発信 SMTP 接続、および DMZ インターフェイスへのバインドを可能にするために、アクセス リスト（この例では **dmz_int) を設定します。**

同様に、メール サーバにアクセスする外部ユーザの場合は、外部ユーザにメール サーバへのアクセスを許可し、アクセス リストを外部インターフェイスにバインドするために、スタティック NAT およびアクセス リスト（この例では **outside_int**）を設定します。

ASA の設定

このドキュメントでは、次の設定を使用しています。

ASA の設定

```
ASA#show run
: Saved
:
ASA Version 8.3(1)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet1
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet2
 no nameif
 no security-level
 no ip address
!
!--- Configure the inside interface. interface Ethernet3
nameif inside security-level 100 ip address 10.1.1.1
255.255.255.0 ! !--- Configure the outside interface.
interface Ethernet4 nameif outside security-level 0 ip
address 192.168.200.225 255.255.255.224 ! !--- Configure
dmz interface. interface Ethernet5 nameif dmz security-
level 10 ip address 172.16.31.1 255.255.255.0 ! passwd
2KFQnbNIdI.2KYOU encrypted boot system disk0:/asa831-
k8.bin ftp mode passive !--- This access list allows
hosts to access !--- IP address 192.168.200.227 for the
SMTP port. access-list outside_int extended permit tcp
any host  192.168.200.227 eq smtp
!--- Allows outgoing SMTP connections. !--- This access
list allows host IP 172.16.31.10 !--- sourcing the SMTP
port to access any host. access-list dmz_int extended
permit tcp host 172.16.31.10 eq smtp any

pager lines 24
mtu BB 1500
mtu inside 1500
mtu outside 1500
mtu dmz 1500
no failover
no asdm history enable
arp timeout 14400


  object network obj-192.168.200.228-192.168.200.253
   range 192.168.200.228-192.168.200.253
 object network obj-192.168.200.254
   host 192.168.200.254
```

```
 object-group network nat-pat-group
   network-object object obj-192.168.200.228-
192.168.200.253
   network-object object obj-192.168.200.254

 object network obj-10.1.1.0
   subnet 10.1.1.0 255.255.255.0
   nat (inside,outside) dynamic nat-pat-group

!--- This network static does not use address
translation. !--- Inside hosts appear on the DMZ with
their own addresses. object network obj-10.1.1.0
   subnet 10.1.1.0 255.255.255.0
   nat (inside,dmz) static obj-10.1.1.0

!--- This network static uses address translation. !---
Hosts that access the mail server from the outside !---
use the 192.168.200.227 address. object network obj-
172.16.31.10
   host 172.16.31.10
   nat (dmz,outside) static 192.168.200.227
access-group outside_int in interface outside
access-group dmz_int in interface dmz
route outside 0.0.0.0 0.0.0.0  192.168.200.226 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
!--- The inspect esmtp command (included in the map)
allows !--- SMTP/ESMTP to inspect the application.


policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
!--- The  inspect esmtp  command (included in the map)
```

```
allows !--- SMTP/ESMTP to inspect the application.

service-policy global_policy global
Cryptochecksum:2653ce2c9446fb244b410c2161a63eda
: end
[OK]
```

ESMTP TLS の設定

注：Transport Layer Security(TLS)暗号化を電子メール通信に使用する場合、ASAのESMTPインスペクション機能（デフォルトで有効）はパケットをドロップします。TLS が有効な電子メールを許可するには、次の出力のように ESMTP インスペクション機能を無効にします。詳細については、Cisco Bug ID CSCtn08326（登録ユーザ専用）を参照してください。

```
ciscoasa(config)#
policy-map global_policy
ciscoasa(config-pmap)#class inspection_default
ciscoasa(config-pmap-c)#no inspect esmtp
ciscoasa(config-pmap-c)#exit
ciscoasa(config-pmap)#exit
```

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

トラブルシューティングのためのコマンド

アウトプット インタープリタ ツール（登録ユーザ専用）（OIT）は、特定の show コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

- debug icmp trace — ホストからの Internet Control Message Protocol（ICMP）要求が ASA に到達するかどうかを示します。このデバッグを実行するには、**access-list コマンドを設定に追加して、ICMP を許可する必要があります。注：このデ**バッグを使用するには、次の出力に示すように、`access-list outside_intICMP`してください。
  ```
  access-list outside_int extended permit tcp any host  192.168.200.227 eq smtp
  access-list outside_int extended permit icmp any any
  ```
- logging buffered 7 — 適応型セキュリティ アプライアンス（ASA）による、ログ バッファへの Syslog メッセージの送信を可能にするためにグローバル コンフィギュレーション モードで使用されます。ASA ログ バッファの内容は、show logging コマンドを使用して確認できます。

ロギングの設定方法の詳細については、「ASDM を使用した Syslog の設定」を参照してください。

関連情報

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- Requests for Comments (RFCs)
- テクニカル サポートとドキュメント – Cisco Systems